TITLE:	MOBILE COMPUTING		
POLICY #:	P-CCSP-018	**EFFECTIVE DATE:**	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	**SUPERCEDES:**	FIRST RELEASE

State of Colorado
Cyber Security Policies

Mobile Computing

THE ENCLOSED POLICIES AND PROCEDURES ARE FOR OFFICIAL USE ONLY WITHIN THE STATE OF COLORADO. THE MATERIAL MAY NOT BE COPIED OR REDISTRIBUTED WITHOUT THE PERMISSION OF THE CISO FOR THE STATE OF COLORADO.

Overview

This policy document is part of the State of Colorado Cyber Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). All Agencies within the scope of this Policy must support and comply with the Requirements section of this document. Additional best-practice guidance is outlined in the Guidelines Section which has been developed help an Agency achieve the objective of this Policy.

For the purposes of this document, an “Agency” includes organizations as defined in C.R.S .24-37.5-102(5).

Authority

C.R.S. 24-37.5-401(1), C.R.S. 24-37.5-403(2)(b)-(c), C.R.S. 24-37.5-404(2)(b).

Scope

This policy document applies to every State agency ("Agency") as defined in C.R.S. 24-37.5-102(5). "State agency" means every state office, whether legislative, executive, or judicial, and all of its respective officers, departments, divisions, commissions, boards, bureaus, and institutions. "State agency" does not include State-supported institutions of higher education, the department of higher education, the Colorado commission on higher education, or other instrumentality thereof.

Policy

All Agencies shall define policies for mobile computing that provide for the protection of sensitive State data.

Definitions

Mobile Computing: A Mobile computing device is any device that is capable of storing and processing information and is intended to be transported outside of a designated state agency office.

Mobile Storage Device: A Mobile storage device is any device that is capable of storing but not processing information and is intended to be transported outside of a designated state agency office.

For the purposes of this document, please refer to C.R.S. 24-37.5-102, C.R.S. 24-37.5-402 and the Colorado Cyber Security Program Policy Glossary for any terms not specifically defined herein.

Roles and Responsibilities

Agency Chief Information Officer (CIO) – is responsible for:

- Defining, maintaining, and enforcing written procedures for mobile computing.
- Supporting the implementation and maintenance of the policy requirements with appropriate budget for staff and IT resources

Agency Information Security Officer (ISO) – is responsible for overseeing that the requirements in this policy are upheld.

Agency IT Staff – is responsible for administering and supporting the technical requirements of this policy, including reporting to the Agency CIO and ISO.

Requirements

All agencies shall create, maintain and implement policies that address the following requirements for mobile computing.

- All agencies are to create and maintain an inventory of mobile computing devices within their control.
- The loss or theft of a State mobile computing or storage device is to be reported to the Information Security Operations Center (ISOC) as a security incident.

Encryption

- All sensitive State information stored on mobile computing or storage devices is to be encrypted whenever the device leaves a State agency office.
- All mobile computing devices that store sensitive information are to employ full disk encryption requiring pre-boot authentication.
- Remote connectivity from a mobile computing device via the internet or leased line is to use Virtual Private Network (VPN) technology to ensure that data is encrypted across publicly-switched networks.
- All mobile computing devices capable of using encryption for network communication are to do so when connected wirelessly to a State network. Devices not capable of using encryption are not to be connected wirelessly to the State network or to any device attached to a state network.

Access Control

- Mobile computing devices are to be configured to use access controls as required by the Access Control Policy, P-CCSP-008.
- When connecting wirelessly to a State network from a mobile computing device the connection is to be authenticated and encrypted according to Wireless Security Policy, P-CCSP-019.
- All mobile computing devices are to be equipped with a "personal firewall" and anti-virus software.

Application Security

- Each agency shall create a process for ensuring mobile computing devices are kept up-to-date with Operating System (OS) and application patches, anti-virus definitions and firewall rule sets.

Guidelines

This section describes best practices for meeting the objective of this policy.

Encryption

- All mobile devices capable of doing so are to use an IPSec encryption and two-factor authentication for communication across VPNs.
- VPNs are not to use split-tunneling mode while connected to a state network.

Access control

- Firewall software on mobile computing devices is to be configured to allow only communication to their Agency's network and VPN endpoint.

Application Security

- Mobile computing devices are to be patched with OS and application updates on the same schedule as other systems on the agency's network.
- Agencies are to deploy VPN technology capable of performing client compliancy checks and of denying access to mobile computing devices that do not have up-to-date patches and anti-virus definitions.

References

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-48, "Wireless Network Security: 802.11, Bluetooth, and Handheld Devices"
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-77, "Guide to IPSec VPNs"

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, “Recommended Security Controls for Federal Information Systems”

- Access Control Policy, P-CCSP-008.

- Cyber Security Planning Policy, P-CCSP-001.